DEPARTMENT OF DEFENSE

DEVELOPING SCIENCE & TECHNOLOGIES LIST

SECTION 17: INFORMATION SECURITY TECHNOLOGY

February 2006

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics
Washington, D.C.

PREFACE

A. THE MILITARILY CRITICAL TECHNOLOGIES PROGRAM (MCTP)

The MCTP supports the development and promulgation of the congressionally mandated Militarily Critical Technologies List (MCTL) and the Developing Science and Technologies List (DSTL).

Congress assigns the Secretary of Defense the responsibility of providing a list of militarily critical technologies (the MCTL) and of updating this list on an ongoing basis. The MCTL identifies technologies crucial to weapons development and has been a key element in evaluating U.S. and worldwide technological capabilities. The MCTP has provided the support for a wide range of assessments and judgments, along with technical justifications for devising U.S. and multilateral controls on exports. The DSTL, another MCTP product, identifies technologies that may enhance future military capabilities.

The MCTP technology assessment process is a continuous analytical and information-gathering process that refines information and updates existing documents to provide thorough and complete technical information. It covers the worldwide technology spectrum and provides a systematic, ongoing assessment and analysis of technologies and assigns values and parameters to these technologies.

Technology Working Groups (TWGs), which are part of this process, provide a reservoir of technical experts. TWG chairpersons continuously screen technologies and nominate items to be added or removed from the list of militarily critical technologies. TWG members are subject matter experts (SMEs) from the military Services, DoD and other federal agencies, industry, and academia. A balance is maintained between public officials and private-sector representatives. Working within an informal structure, TWG members strive to produce precise and objective analyses across dissimilar and often disparate areas. Currently, the TWGs are organized to address 20 technology areas:

Aeronautics

Armament and Energetic Materials

Biological

Biomedical

Chemical

Directed Energy Systems

Electronics

Energy Systems

Ground Combat Systems

Information Security

Information Systems

Lasers, Optics, and Imaging

Processing and Manufacturing

Marine Systems

Materials and Processes

Nuclear Systems

Positioning, Navigation, and Time

Signature Control

Space Systems

Weapons Systems

B. THE DEVELOPING SCIENCE AND TECHNOLOGIES LIST (DSTL)

The DSTL focuses on worldwide government and commercial scientific and technological capabilities that have the potential to significantly enhance or degrade US military capabilities in the future. It includes new and enabling technologies as well as those that can be retrofitted and integrated because of technological advances. It assigns values and parameters to the technologies and covers the worldwide technology spectrum.

The DSTL is oriented towards advanced research and development including science and technology. It is developed to be a reference for international cooperative technology programs. The DSTL includes basic research, applied research and advanced technology development. Separate documents contain a Glossary and a list of Acronyms and Abbreviations.

This document, DSTL Section 17: Information Security Technology supersedes DSTL, Section 10.4, Information Security Technology, May 2000.

INTRODUCTION

A. ORGANIZATION OF THE DEVELOPING SCIENCE AND TECHNOLOGIES LIST (DSTL)

The DSTL is a documented snapshot in time of the ongoing MCTP technology assessment process. It includes text and graphic displays of technical data on individual technology data sheets.

Each section contains subsections devoted to specific technology areas. The section front matter contains the following:

- *Scope* identifies the technology groups covered in the section. Each group is covered in a separate subsection.
- *Highlights* identify the key facts in the section.
- *Overview* discusses the technology groups identified under “Scope.”
- *Background* provides additional information.

Each technology group identified under Scope has a subsection that contains the following:

- *Highlights* identify the key facts found in the subsection.
- *Overview* identifies and discusses technologies listed in data sheets that follow.
- *Background* provides additional information.
- *Data Sheets,* which are the heart of the DSTL, present data on individual technologies.

B. TECHNOLOGY DATA SHEETS

The technology data sheets are of primary interest to all users. They contain the detailed parametric information that managers, R&D personnel, program managers (PMs), and operators need to execute their responsibilities.

- *Technology Parameter(s)* includes the parameter, data argument, value, or level of the technology where it might have the potential to significantly enhance or degrade US military capabilities in the future.
- *Critical Materials* are those materials that are unique or enable the capability or function of the technology.
- *Unique Test, Production and Inspection Equipment* includes that type of equipment that is unique.
- *Unique Software* is software needed to produce, operate, or maintain this technology that is unique.
- *Major Commercial Applications* addresses commercial uses of this technology.
- *Affordability Issues* are those factors that make this technology an affordability issue.
- *Background* provides additional information.

SECTION 17—INFORMATION SECURITY TECHNOLOGY

Scope

Highlights

- Strong personnel, facilities, equipment, standardization, training, and test and evaluation (T&E) security programs as well as defensive information operations and operations security are key components of secure militarily critical information and infrastructure assurance systems.
- Commercial information security technologies, techniques, and products are widely available in world markets and have adequate capabilities for the protection of some militarily critical information systems in commercial-off-the-shelf (COTS) versions, many of which can be customized by adversaries, rogue states, subnational groups, terrorists, criminals, and international crime syndicates.
- A large number of countries have academic communities and elements that understand this technology and develop, produce, or use this technology.
- Significant progress is being made in the development of open, market-based information security products. These products include commercial public key infrastructures (PKIs) and cryptographic, steganographic, biometric, and software security systems, many of which are now covered by national and international standards and national and international security export controls.
- In the Information Age, few computers are not connected to the Internet or some form of network. Single-channel signaling and operating systems that can be hacked make firewalls between computers and the Internet a necessity.
- Unreliable software and malware (software designed to infiltrate or damage a computer system, without the owner’s consent) are significant threats to information systems.
- Potential adversaries of the United States have the same access to the global commercial industrial base and installed communications base, including some of the same information security technologies and products that the U.S. military forces have.
- Protection is critical for United States Government (USG) intellectual property and next-generation weapon system scientific, empirical systems engineering and integration (SE&I), modeling and simulation (M&S) applications, and data.
- Open, worldwide information security research and development (R&D) is producing technologies (which have undergone international open scientific peer review) that are enabling the development of sound militarily critical information and national security information assurance security systems.
- Armed forces are transitioning to Network Centric Warfare (NCW), which will place added emphasis on information security.

OVERVIEW

Information security is far more than the technologies and products identified in this section. Many other information-security-related computer software and hardware, facility, and equipment technologies—all of which are important to the security of military information systems and the National infrastructure—are still in the investigation or development stage. However, most of these technologies are widely understood and nationally and internationally known. Information security technologies are closely related to those in the areas of information technology (Section 10) because information security modules, components, and systems must be tightly integrated with, if not an integral component or module of, the basic information processing hardware and software architecture, which must be integrated and tested during system development.

Essentially, all the information security technologies and products require or will require unique, empirically validated SE&I experience and related techniques and software during their development, production, and operational life cycle. Producing information dominance systems for U.S. forces would not be possible without the information security product manufacturer's SE&I know-how.

Many applications now incorporate high-performance features and metaprocessing techniques that are shortening the cryptanalytic time required for an exhaustive key search, which makes *information processing* technologies closely related to the technologies [especially the high performance computing (HPC) technologies] addressed in this section. The length of time required for cryptanalyses is a function of knowledge in the field of mathematics and the state of the art in HPC. Processing power determines the length of time required to perform an exhaustive key search, which, in turn, governs the life cycle for key lengths.

Identity management technologies are closely related to the access and circulation control system technologies that protect sensitive facilities, equipment, and data. Some telecommunications technologies, such as the spread spectrum and frequency hopping technologies commonly used in civilian and military cellular telephone systems, are closely related. They now normally incorporate cryptographic modules to protect the dialing and billing codes over radio frequency (RF) links. The networks and switching technologies in the links and nodes of the switched network information communications systems are also closely related. For example, link encryption (usually some form of stream encryption) is used to protect the commercial backbone links in the installed base.

Information security technologies are also closely related to the tracking, telemetry, and control (TT&C) encryption and decryption technologies for military systems and some positioning, navigation and time technologies (Section 16). The commanding uplinks and mission data downlinks for some civilian satellites and for all military satellites [e.g., the Global Positioning System (GPS)] are protected by encryption to maintain positive control of the satellite systems and prevent mission data interception, intrusion, and spoofing.

The Wassenaar Arrangement countries define "Information Security" as follows:

> *All the means and functions ensuring the accessibility, confidentiality, or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes cryptography, cryptanalysis, protection against compromising emanations, and computer security.*[1]

Information Security is National Security:

> *Now we are in the Information Age. Whole national economies are being restructured around the exploitation of information, and other aspects of societies are following suit. Militaries also are redefining their capabilities around related technologies. Data is the lifeblood of these digital societies, and interruptions of that essential information flow could have grave consequences for the health of a nation. Consequently, the blunt fact is that* ***Information Security is National Security****. No longer merely a subset of a larger issue, Information Security is now the primary issue about which the free world must be concerned.*[2]

[1] The *Wassenaar Arrangement List of Dual-Use Goods and Technologies* and *Munitions List*, WA-LIST (05) 1, 12-14-05 (http://www.wassenaar.org/list/wa-listTableOfContents.htm).

[2] Lt. Gen. C. Norman Wood, USAF (Retired) in the President's Commentary, *SIGNAL*, August 2001, p. 14.

Information security technologies are essential for the protection of the critical National infrastructure and cyber attack risk management.

> *Terrorists may seek to cause widespread disruption and damage, including casualties, by attacking our electronic and computer networks, which are linked to other critical infrastructures such as our energy, financial, and security networks. Terrorist groups are already exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely. As terrorists further develop their technical capabilities and become more familiar with potential targets, cyber attacks will become an increasingly significant threat.*[3]

The diffusion of information technology and advanced communications has shaped the face of modern international terrorism and how terrorists operate, affecting their menu of possible methods of operation.

> *The concern about "cyberterrorism" is so recent because both the accessibility of relevant technology and the range of systems potentially vulnerable to electronic attack have expanded so fast. The concern about chemical, biological, radiological, or nuclear (CBRN) terrorism is based partly on the increased ease of finding pertinent technical information on an exponentially expanding Internet.*[4]

Human frailty, although not covered in depth in this section, still accounts for roughly 75 to 80 percent of the information security system failures, as it has for the last 30 years. Therefore, the key link in any information security chain is not a technology per se; rather, it is the people who manage and use information security system operations. Technology can reduce, but not eliminate, the human frailty risks to trusted information systems. *The Register* has reported[5] that a 2003 Computing Technology Industry Association (CompTIA) survey found that human error alone was the cause of 63 percent of security breaches. The latest survey, identified in 2004,[6] indicates a significant increase in human error. Eighty-four percent of the 900 respondents said that human error was either wholly or partially to blame for their last major security breach.

The greatest security risk reduction requirement is, perhaps, to monitor more carefully selected security system management, operation, and administration functions and to recruit personnel who have better qualifications and skill matches for the sensitive information security systems areas in which they work. Equally important are more careful selection and training of security information system managers and end users. In short, all personnel who manage, operate, administer, and use secure information systems must be capable individuals who understand completely the high trust and great responsibility necessary to work in the information security systems area. Improvements in the number and quality of personnel selected to manage and use information security systems must be combined with vigorous security indoctrination and training, including a thorough training program in operations security, procedures standardization, and recurrent tests, exercises, and evaluations.[7]

BACKGROUND

Cryptology presents the same difficulty found in all classic scientific disciplines: the need for a continuous challenge and response interaction between cryptographers and cryptanalysts. This scientific interaction begins with a challenge from cryptographers, which starts each cycle with a new algorithm design, and a response from the cryptanalysts through continuing open scientific peer review. Scientists in this field search for flaws in the algorithm. During these peer reviews and the continuous study of new cryptographic systems, the cryptanalysts try to find and expose design flaws, which is usually harder than designing the cryptographic algorithms. The result of

[3] *National Strategy for Homeland Security*, Office of Homeland Security, July 2002, p. 9.

[4] Paul R. Pillar, *Terrorism and U.S. Foreign Policy*, Brookings Institution Press, Washington, DC, 2001, p. 47.

[5] *The Register*, 1 April 2004, Updated:1330 GMT. http://www.theregister.co.uk/content/55/36706.html.

[6] Steve Gold, Human Error To Blame for Most Security Breaches, *The SC Infosecurity Newswire*, Week Ending April 2, 2004, http://www.infosecnews.com.

[7] The Interagency Operations Security Staff (IOSS) provides operations security products and services free of charge to the government and its supporting contractors. A complete set of operations security training materials is available through http://www.ioss.gov/ or by e-mail from ioss@radium.ncsc.mil.

the evolutionary struggle in this open scientific peer review method is a healthy, competitive public testing process that produces strong cryptography[8] (see Figure 17.0-1).

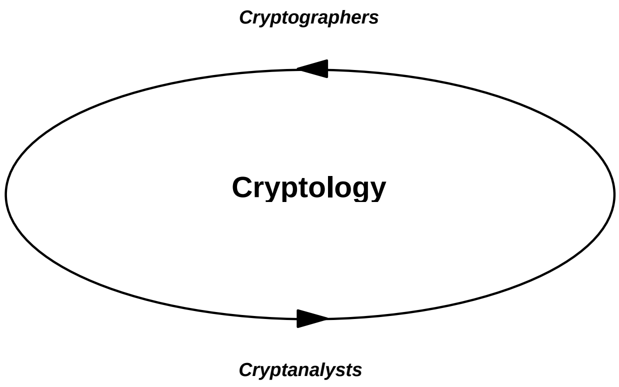

Figure 17.0-1. The Open Publication and Public Cryptanalytic Testing Process Provides the Insight Necessary for Designing Strong Cryptography

Over the centuries, the ongoing battle between cryptographers and cryptanalysts has inspired a whole series of remarkable scientific breakthroughs, as cryptographers have striven to construct ever-stronger cryptographic designs and cryptanalysts have continually invented more powerful methods of analysis. Matt Blaze's declaration for the Recording Industry Association of America, Inc., copyright case[9] is a concise explanation of the value of scientific openness and the peer review process to cryptologic evolution:

> *It should not be surprising, as paradoxical as it may seem at first blush, that researchers and other scientists who study security and privacy customarily embrace and value openness and wide publication even of results that expose vulnerabilities. Such publication represents the natural advance of knowledge in a relatively new field of scientific study.*

Bruce Schneier's observation is more to the point:

> *A basic rule of cryptography is to use published, public algorithms and protocols. This principle was first stated in 1883 by Auguste Kerckhoffs (1835–1903): "In a well-designed cryptographic system, only the key needs to be secret; there should be no secrecy in the algorithm."*[10]

Information security is generally regarded as an essential functional area, system segment, or feature of all military information systems and most civilian systems, which require unique, empirically validated SE&I

[8] Cryptography and cryptographic devices and the technical data associated with them are subject to federal export controls, unless exempt. Exports of cryptographic modules that implement the specified standard and technical data regarding them must comply with these federal regulations and be licensed by the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce (DOC), as required. Applicable federal government export controls are specified in: Title 15, Code of Federal Regulations (CFR) Part 740.17; Title 15 CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.

[9] Grayson Barber (GB 0034), Grayson Barber, L.L.C., 68 Locust Lane; Princeton, New Jersey 08540; (609) 921-0391; Frank L. Corrado (FLC 9895); Rossi, Barry, Corrado, and Grassi, 2700 Pacific Avenue Wildwood, NJ 08260 (609) 729-1333; Attorneys for Plaintiffs. IN THE UNITED STATES DISTRICT COURT, FOR THE DISTRICT OF NEW JERSEY. EDWARD W. FELTEN; BEDE LIU; SCOTT A. CRAVER; MIN WU; DAN S. WALLACH; BEN SWARTZLANDER; ADAM STUBBLEFIELD; RICHARD DREWS DEAN; and USENIX ASSOCIATION. Hon. Garrett E. Brown, Jr., a Delaware non-profit non-stock Case No. CV-01-2669 (GEB) corporation, Civil Action. Plaintiffs. vs. RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.; SECURE DIGITAL MUSIC INITIATIVE FOUNDATION; VERANCE CORPORATION; JOHN ASHCROFT, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES; DOES 1 through 4, inclusive, Defendants. DECLARATION OF MATTHEW BLAZE. http://www.salon.com/tech/log/2001/08/31/dmca_animals/index.html. 9/22/2001 8:56 AM.

[10] Bruce Schneier, *CRYPTO-GRAM*, Counterpane Internet Security, Inc., schneier@counterpane.com, http://www.counterpane.com.

experience, related techniques, and software during the development, production, and operational life cycle of the information security segments in secure information systems. The information technology life cycle is typically described in five phases:

1. Initiation (requirements generation)
2. Development/acquisition
3. Implementation
4. Operations/maintenance
5. Disposal.

SECTION 17.1 – CRYPTOLOGY

Highlights

- The security of cryptographic algorithms is always at risk of disproof by the next cryptanalytic attack.
- The strength[11] of encryption algorithms is based on assumptions and inferences about the hardness of mathematics problems on which the algorithm is based.
- *Mathematics,* in general, and cryptology, in particular, are the basis for the emerging strong dual-use cryptographic functions, applications, and systems worldwide.
- *Distributed key generation* (DKG) is fundamental to meeting the requirement for secure, scaleable cryptographic systems.
- In many *DKG* contexts, it is impractical or impossible to assume that a trusted third party (TTP) is present to generate and distribute key shares to users in the system. In essence, DKG allows a set of players to generate a public/private key pair collectively, with the "shares" of the private key spread over the players so that any sufficiently large subset can reveal or use the key.
- *Elliptic Curve Cryptography*[12] (ECC) offers high efficiency and low overhead for encryption, digital signatures, and key management applications because of its presumed strength, with shorter keys and higher processor efficiency.
- The security of cryptography depends on *random numbers*. The difficult part is obtaining the random numbers. There is no way to prove that a number is truly random.
- *Stream ciphers* are more appropriate and, in some cases, mandatory for telecommunications applications and other applications when buffering is limited or when characters must be individually processed as they are received. They have limited or no error propagation and are especially well suited in situations where transmission errors are highly probable.
- Various design principles of *stream ciphers* have been proposed, and a few have been extensively analyzed; however, few have proofs and a careful estimate of cryptographic strength.
- Although at least three countries produce commercial *quantum cryptography* products that are, or soon will be, on the market, *quantum cryptography* will remain in the scientific investigation phase for many years. There are many challenges (e.g., range) ahead.

OVERVIEW

The cryptology technologies in this section specify those identified scientific investigations and developing technologies that are largely cryptographic in nature, as differentiated from the protocols and techniques associated with cryptographic functionality in secure information processing systems. They are in the public domain. Some are now widely available in the world market but are forecast to be developing in the period beyond the next 5 years.

[11] The metric for cryptographic *strength* is *key length*, which determines the *time* and *resources* required to perform an exhaustive key search and, in turn, the effective *life cycle* of a key.

[12] Cryptography, cryptographic devices, and technical data regarding them are subject to federal export controls, unless exempt. Exports of cryptographic modules implementing the specified standard and technical data regarding them must comply with federal regulations and be licensed by the BIS of the U.S. DOC, as required. Applicable federal government export controls are specified in Title 15, CFR Part 740.17; Title 15 CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.

BACKGROUND

Cryptology[13] is the generally recognized collective term used by the cryptologic community for cryptography, cryptanalysis, and related protocols and techniques. The Joint Staff [Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*] defines cryptology as

> *…the science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.*

Cryptography[21] is composed of two basic elements:

1. An algorithm (or cryptographic methodology)
2. A key.

Algorithms are complex mathematical formulae, and, in the digital age, keys are strings of binary digits or "bits."[14] The same algorithm or algorithms that are designed to work together must be used for encryption and decryption. The strength of encryption algorithms is based on assumptions and inferences about the hardness of the mathematics problems on which the algorithm is based. For that reason, encryption can never be proven to be unbreakable or unconditionally secure as long as these assumptions and inferences are believed. An algorithm can be proven to be insecure by successfully attacking (breaking) the ciphertext and recovering the cleartext, which happens from time to time. Until broken, most encryption algorithms are provisionally accepted as "strong" if they have undergone extensive international peer review in the public domain. The longer these algorithms are under peer review in the public domain, the greater the confidence in their strength and the truth of the assumptions and inferences about the hardness of their underlying mathematics problems.

The security of a cryptosystem must not depend on keeping the cryptographic algorithm secret[15] because history suggests that eventually a secret algorithm is sure to be discovered independently by someone else or be stolen. Therefore, the security of strong cryptography must depend on the length of the key. Generally, the longer the keys, the more secure the cryptography.

If a cryptographic algorithm is sound and no shortcut solutions can be found, performing an exhaustive key search will take more time if the key is long. With the present knowledge of mathematics and state-of-the-art processor strength, an exhaustive key search becomes computationally infeasible at some key length. For these reasons, the objective numeric metric scale for specifying cryptographic "strength" is now graduated in key lengths, and life-cycle forecasts are specified in key lengths required in future years.

The longer cryptographic algorithms remain in the public domain under international peer review and remain unbroken, the stronger they are assumed to be. However, the possibility always exists that a new attack or a breakthrough in mathematics will make the solution of the underlying problem faster and easier. Also, the possibility of a sudden order-of-magnitude increase in processing power exists, which shortens the time required for an exhaustive key search to the point that the cryptographic algorithm does not provide protection of encrypted data for the required length of time.

To provide a high level of security for any information system, encryption algorithms (no matter how strong) must be integrated during system development—running on secure platforms that also have sound protocols, authentication, and secure links to secure nodes.

[13] *Cryptology* is a *field* of mathematics based on algorithms that perform calculations to encipher and decipher text, files and data. Cryptography is the art and science of keeping messages secure, is practiced by cryptographers. *Cryptography* was derived from two ancient Greek words: *kryptos*, meaning hidden, and *graphia*, meaning writing. [Source: Schneier, Bruce, *Applied Cryptography*: *Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995, p. 1.] Cryptography can provide confidentiality (or secrecy) and authentication and verify the integrity of data and the identity of the originator(s).

[14] A bit is a binary digit: 1 or 0.

[15] Simon Singh, *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, New York, 1999, p. 12.

Projections for the useful life of cryptologic technologies are difficult because of the many unknowable variables in mathematics and computer science, both of which control the future of these technologies. The only reasonable generalized projection that could be made about the rate of change in these technologies is that the rate of change in cryptologic technologies might be forecast as “slow” and processing power as comparatively rapid in the future.

Notable exceptions to these general rules may be quantum computers and quantum cryptography. Many authorities had predicted that at least 25 years would pass before any form of quantum cryptography would have practical utility. Although three manufacturers now have quantum cryptography products on the market, quantum cryptography still will be a developing technology for many years and faces many challenges (e.g., range) in the future. Conventional cryptography will be needed for many years and probably will never be completely replaced by quantum cryptography.

Some of the latest cryptologic technologies are still the subject of continuing scientific investigation or are in R&D, even though there are early commercial products. Standards are being developed for some of these new technologies. In the increasingly competitive Information Age, with the Internet to spread knowledge rapidly, protecting U.S. intellectual property and next-generation weapon systems, empirical SE&I, M&S applications, and technical data has become critical.

Cryptologic scientific investigations and developing technologies are closely related to those in the area of information technology (Section 10) because information security modules, components, and systems must be tightly integrated with, if not an integral component or module of, the basic information processing hardware and software architecture.

Many applications now incorporate high-performance features and metaprocessing techniques that are shortening the cryptanalytic time required for an exhaustive key search. The length of time required for cryptanalyses is a function of knowledge in the field of mathematics and the state of the art in HPC.

Cryptanalytic procedures and techniques are largely dependent on the state of the art in HPC because processing power is still increasing rapidly, and, therefore it determines the length of time required to perform an exhaustive key search. This, in turn, governs the life cycle of some algorithms and most key lengths.

LIST OF DSTL TECHNOLOGY DATA SHEETS
17.1. CRYPTOLOGY

DSTL DATA SHEET 17.1-1. MATHEMATICS

Mathematics is the basic science of arithmetic (numbers and their operations, interrelations, combinations, generalizations, and abstractions) and geometry (space configurations and their structure, measurement, transformations, and generalizations).

Technology Parameter(s)	Science and technology discoveries in mathematics that (1) Have the potential to enhance or degrade significantly the current U.S. military communications intelligence (COMINT) cryptographic and cryptanalytic capabilities and (2) Have the potential to enhance or degrade significantly the existing U.S. commercial dual-use and U.S. Suite A or Suite B cryptographic algorithms, applications, or protocols in the future.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Software required to investigate cryptographic and cryptanalytic capabilities.
Major Commercial Applications	Mathematics, in general, and cryptology, in particular, are the basis for products in the financial services industry, telecommunications industry, and legal and medical services. Developers of a wide variety of e-commerce applications and personal privacy products drive this technology.
Affordability Issues	Because of the expensive and time-consuming effort required for mathematics and cryptologic investigations and discoveries, research is most likely to be financed by nation states, industry, or well-financed universities or independent groups.

BACKGROUND

Mathematics is the study of relationships using numbers and the study of the relationships among numbers, shapes, and quantities. It uses signs, symbols, and proofs and includes algebra, calculus, and trigonometry.

Cryptology is a specialized field of applied mathematics. It is based on algorithms that perform calculations to encipher and decipher, provide integrity for, and digitally sign text, files, data and the ways to attack such algorithms. Various forms of cryptology have been in the public domain for centuries, and cryptology is now widely studied by nation states, industry, and academia. Number theory and discrete mathematics are important areas in this field.

DSTL DATA SHEET 17.1-2. DISTRIBUTED KEY GENERATION (DKG)

DKG is used to initialize a cryptosystem and generate its private and public keys. It is also used as a subprotocol (e.g., to generate a one-time key pair), which is a part of any threshold El-Gamal-like signature scheme.

Technology Parameter(s)	(1) New scientific investigation and research results that have the potential to enhance or degrade significantly the DKG capabilities; (2) Early results of basic and applied research and advanced basic and applied research in DKG schemes; (3) Prototypes of advanced technology key generation models; (4) Scientific investigation and research findings in failure mode and effects analyses of DKG systems; (5) Has reproducible results that have the potential to enhance or degrade significantly the current U.S. military and dual-use DKG capabilities; and (6) Has the potential to enhance or degraded significantly the existing DKG capabilities for USG Suite A or Suite B cryptographic systems.
Critical Materials	None identified**.**
Unique Test, Production, Inspection Equipment	None identified**.**
Unique Software	Software required to test DKG capabilities.
Major Commercial Applications	The information security industry supplies DKG commercial applications to the financial services industry, telecommunications industry, legal and medical services, and developers of a wide variety of e-commerce applications and personal privacy products. The threats from independent hackers and crackers and those from nation states, rogue states, terrorists, and international criminals drive this technology.
Affordability Issues	Because of the expensive and time-consuming scientific investigations, basic and applied research is most likely to be financed by nation states or universities.

BACKGROUND

DKG allows a set of players to generate collectively a public/private key pair, with the “shares” of the private key spread over the players so that any sufficiently large subset can reveal or use the key. The generated key pair is then used in a discrete, log-based cryptosystem. Commonly, the security parameter of such a system is called the threshold, ***t***. This is the number of players who can be corrupted without the key being compromised.

A sound PKI is one of the most critical elements of a DKG protocol. National and international standards bodies are working on PKI issues. The Federal Public Key Infrastructure (FPKI) Technical Working Group is moving to develop a standard for USG certificate management. A robust PKI that supports DKG is a dual-use item that could be used by governments and military forces.

DSTL DATA SHEET 17.1-3. ELLIPTIC CURVE SYSTEM SECURITY

Elliptic Curve System Security uses ECC, which is an approach to cryptography based on the mathematics of elliptic curves.

Technology Parameter(s)	(1) Proof of ECC[16] system security; (2) Has undergone extensive, open scientific peer review, with no short-cut attacks discovered; and (3) Has at least 256-bit key spaces for ECC systems.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed to support randomness; Multiple Polynomial Quadratic Sieve (MPQS), double large prime variation of the MPQS, Number Field Sieve (NFS) factoring and discrete log (e.g., index-calculus algorithms for use in asymmetric system development, testing, quality control, and evaluation); software specially designed to support Pollard's parallel collision and Koblitz tests for the security of ECC systems.
Major Commercial Applications	Financial services industries, Internet, e-commerce, and business network operators have been the principal open-source drivers of elliptic curve technologies in recent years. While commercial cryptographic applications may not yet equal the strength of some government systems, the gap between the strength of government and civilian systems seems to be closing. In large part, the strength gap may be closing because of the national and international open peer review scientific methods now in use and the significant R&D investments being made by the information systems industry world-wide. Elliptic curve applications are ideally suited to system segments that have limited power, small bandwidths, and limited storage and processor capacities.
Affordability Issues	Competitive, information system security COTS products are appearing in the open market, with strong elliptic curve asymmetric cryptographic functionality, at little or no additional cost. However, the cost of security indoctrination and additional staff needed to manage and maintain secure cryptographic functionality for large complex systems is a significant cost issue, even though most of the secure cryptographic processes can be automated. Even after automation, there is still a potentially expensive requirement to recruit and retain technically qualified, responsible, trustworthy personnel and to operate, manage, and support the required end-user training, standardization, T&E programs required for optimum protocol security and the maintenance of system security.

BACKGROUND

ECC offers high efficiency and low overhead for encryption, digital signatures, and key management applications because of its presumed strength, with shorter keys and high processor efficiency. This dual-use cryptographic technology is maturing rapidly. The principal attraction of ECC, as compared with RSA, is that it offers equal security for a far smaller key size, thereby reducing processing overhead.

ANSI X9.62, *ECDSA (Elliptic Curve Digital Signature Algorithm)* describes a method for digital signatures using the elliptic curve analog of the Digital Signature Algorithm (DSA) [ANSI X9.30.1-1997: *Public-Key Cryptography for the Financial Services Industry - Part 1: The Digital Signature Algorithm (DSA)*]. ECC is a form of public-key (asymmetric) cryptography, whose algorithms are typically used to

[16] Cryptography and cryptographic devices and technical data regarding them are subject to federal export controls, unless exempt. Exports of cryptographic modules implementing the specified standard and technical data regarding them must comply with federal regulations and be licensed by DOC's BIS. Applicable federal government export controls are specified in Title 15, CFR Part 740.17; Title 15 CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.

1. Create digital signatures (in conjunction with a hash algorithm)
2. Establish secret keys securely for use in symmetric-key cryptography.

When implemented with proper controls, the techniques of ANSI X9.31-1998, D*igital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry,* provide

1. Data integrity
2. Data origin authentication
3. Non-repudiation of the message origin and message.

Elliptic curve cryptographic systems are gaining widespread acceptance. Several companies have developed USG Suite A elliptic curve cryptographic systems suitable for the protection of classified information and SBU information.

DSTL DATA SHEET 17.1-4. DETERMINISTIC RANDOM NUMBER GENERATION

A *deterministic random bit generator (DRBG)* consists of an algorithm that produces a string of bits from an initial value called a seed, which is typically supplied from a non-deterministic random bit generator (RBG).

Technology Parameter(s)	Has a physical non-deterministic entropy source that (1) Is unpredictable; (2) Is statistically unique; (3) Has a negligible probability threshold of a successful attack; (4) Is backtracking and prediction resistant; (5) Is one that produces an apparently random sequence of bits from an initial value called a seed, along with possible other inputs, which might even include non-deterministic inputs. The output from the generation is dependent on the contents of the internal state. The same internal state will result in the same output. (A DRBG is often called a pseudorandom number (or bit) generator.); and (6) Ensures conformance by an independent testing laboratory associated with the NIST Cryptographic Module Validation Program (CMVP).
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Commercial drivers are the educational community, statisticians, programmers, scientists, and researchers who use random numbers to conduct “unbiased” experiments.
Affordability Issues	Affordability should not be an issue. The best efforts of the U.S. science and technological community are required continually to develop better techniques for generating deterministic random numbers and proofs of their randomness.

BACKGROUND

The two basic types of generators used to produce random sequences are (1) random number generators (RNGs) and (2) pseudorandom number generators (PRNGs). An RNG uses a non-deterministic source (i.e., some unpredictable physical source) to produce random bits. A PRNG produces a sequence of bits from an initial value called a seed, using a known algorithm and a deterministic computer. Various statistical tests can be applied to a sequence produced by such generators to compare and evaluate the sequence for randomness. The distribution of outcomes of statistical tests, when applied to a truly random sequence, is known a priori and can be described in probabilistic terms. However, no set of statistical tests is sufficient to certify the randomness of a generator. The analysis of the generator’s design (e.g., cryptanalysis) is also required.

There are two basic classes of RBGs:[17]

- A non-deterministic RBG produces output that is dependent on some unpredictable physical source. Other names that are often used for non-deterministic random bit generators are true random number (or bit) generators and, simply, random number (or bit) generators.[18]
- A deterministic RBG consists of an algorithm that produces a string of bits from an initial value called a seed, which is typically supplied from a non-deterministic random bit generator. With a relatively small seed, a deterministic RBG can produce a relatively long non-repeating sequence of bits. The output from the generator is dependent on the value of the seed and any other preset information (e.g., a key, counter, or date). Therefore, the output is determined by the seed and this other information and is predictable if the seed and other information are known. Since the output is predictable in this case, the sequence that is

[17] Under reasonable assumptions, it is not feasible to distinguish the output of the RBG from true random numbers that are uniformly distributed or without replacement. Informally, all possible outputs occur with equal probability, and a series of outputs appears to conform to the uniform distribution.

[18] ANS X9.82, *Random Number Generation: Part 1*, Draft, 16 January 2003, p. vii.

output is not considered to be a truly random sequence, and the generator is often called a *pseudorandom number (or bit) generator*.[19]

ADDITIONAL INFORMATION

A "one-time pad" cryptographic scheme was used by German and Soviet diplomats for their communications before and during World War II and by Communist spies during the Cold War.[20] The name comes from the practice of printing the key in the form of paper pads, each sheet of which is torn out and destroyed after being used just once. The one-time pad is completely secure provided that

- The key's sequence of digits is truly random
- The key, which must be as long as the message, is used only once.

It is the randomness of the key that wipes out any patterns that could be used by code breakers to crack these ciphers. Of course, this assumes perfect key management and security at both ends.

Even though one-time pads are slow and the logistics are cumbersome, they are still used for some special purposes. The parties involved must initially meet to decide on the keys or take the risk of having the key hand-delivered by a trusted courier or transmitted over a telephone. Either way is potentially insecure, especially because the keys are lengthy and must be changed regularly to increase security.

In addition to one-time pads, random or pseudorandom numbers are used in

- Digital signature generation and verification
- The selection process for the prime factors of the modulus and for the public verification exponent for digital signature generation and verification using reversible public cryptographic systems
- The generation of static and ephemeral private keys and the prime moduli
- The derivation of a user's key pair and the creation of masked data that are used to format the payload
- Generating the keys and initialization vectors for the Triple Data Encryption Algorithm (TDEA) modes of operation
- Digital signature generation and verification using elliptic curve techniques
- The generation of elliptic curves, points on the curve, and public key pairs
- Key wrapping
- PIN and password generation
- Quantum cryptography key distribution systems.

[19] ANS X9.82, *Random Number Generation: Part 1,* Draft, 16 January 2003, p. 2.

[20] The one-time pad was also used by the United States Air Force (USAF) after World War II in the Caribbean Air Command to protect the Morse codes messages transmitted over high-frequency (HF) links between headquarters and island bases for priority communications.

DSTL DATA SHEET 17.1-5. MESSAGE INTEGRITY AND NON-REPUDIATION

Message integrity and *non-repudiation* convince a receiver of the identity of the message sender and message integrity. Non-repudiation provides the sender proof of delivery and the recipient assurance of the sender's identity, so that neither can later deny having processed the data.

Technology Parameter(s)	(1) Has undergone extensive, open peer review and no short-cut attacks[21] have been discovered; (2) Has Closed-loop Response Integrity;[22] (3) Has at least 3,072-bit key spaces for Digital Signature Algorithm/Diffie-Hellman (DSA/DH) and RSA systems; (4) Has at least 128-bit key spaces for Message Authentication Codes (MACs); (5) Has a hash value of at least 256 bits for digital signature applications or features; and (6) Has time stamp applications or features using the NIST time[23] signal and is ANSI X9.95[24] compliant.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Message integrity and non-repudiation application software and the operating systems on which it runs must have defects less than least *Six Sigma*[25] and specially designed software to support randomness, MPQS, double large prime variation of the MPQS, NFS factoring, and discrete log (e.g., index-calculus algorithms for use in asymmetric system development, testing, quality control, and evaluation.)
Major Commercial Applications	Financial services industries, Internet, e-commerce, and business network operators.
Affordability Issues	Competitive, information system security COTS products with strong digital signature and asymmetric cryptographic functionality are appearing in the open market at little or no additional cost. However, the cost of security indoctrination and additional staff to manage and maintain secure cryptographic functionality for large complex systems is a significant cost issue.

BACKGROUND

Message integrity:

- The property of ensuring that data are transmitted from source to destination without undetected alteration.[26]
- The property that sensitive data have not been modified or deleted in an unauthorized and undetected manner.[27]

[21] A short-cut solution to the factoring problem or discrete log problem would make most current public key systems obsolete.

[22] Closed-loop Response Integrity is the verification by the originator of the overall transaction integrity (i.e., of both the transaction request and its transaction response). See ANSI X9.19, *Financial Institution Retail Message Authentication.*

[23] See http://www.time.gov (click on "Time Exhibits" and "A Walk Through Time").

[24] ANSI, X9.95-2005, *Trusted Time Stamp Management and Security*.

[25] Six Sigma is a statistical measure of extraordinarily high quality. At Six Sigma, only 3.4 defects per 1 million opportunities will occur.

[26] R. Atkinson, *Network Working Group Request for Comments—1825 Category: Standards Track*, Naval Research Laboratory, August 1995.

[27] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.*

Non-repudiation:

1. Provides proof of the integrity and origin of data that can be verified by a third entity[28]
2. Is the property of a receiver being able to prove that the sender of some data did, in fact, send the data even though the sender might later want to deny having sent that data[29]
3. Is evidence of the identity of the signer[30] of a message and message integrity, sufficient to prevent a party from successfully denying the origin, submission, or delivery of a message and the integrity of its contents[31]
4. Provides the data sender proof of delivery
5. Is the assurance provided to entity ***U*** that ***U*** is able to prove to a third party that data are from ***V***.[32]

Currently, there are three FIPS-approved[33] algorithms for generating and verifying digital signatures: (DSA, RSA,[34] and ECDSA.[35] All three algorithms are used in conjunction with a FIPS-approved hash function (see http://csrc.nist.gov/CryptoToolkit/tkhash.html). *A hash function*[36] hashes and compresses a plaintext message of arbitrary length into a fixed-size digest, or *hash value*.

Most public-key algorithms operate on fixed-size blocks, usually 3,072 bits or larger for RSA™ and the DSA.[37] For applications requiring the authentication of data integrity and the identity of the signer, the DSS[38] is used in conjunction with SHA-1. When using these algorithms to create digital signatures, messages are typically run through a cryptographic hash function, and the output of this function is what is actually signed. This output is called the message digest.

[28] ANSI X9.57-1997, *Public Key Cryptography for the Financial Services Industry: Certificate Management.*

[29] R. Atkinson, *Network Working Group Request for Comments—1825 Category: Standards Track*, Naval Research Laboratory, August 1995.

[30] Signing is the act of encrypting a document with a private key.

[31] *DoD Target PKI User Requirements*, Draft dated 29 February 2000.

[32] ANSI X9.92-2001, *Public Key Cryptography for the Financial Services Industry: PV-digital Signature Scheme Giving Partial Message Recovery (PVS)* [PVS is the Pintsov-Vanstone DSA giving partial message recovery].

[33] A security method (e.g., cryptographic algorithm, cryptographic key generation algorithm, or key distribution technique, authentication technique, or evaluation criteria) that is either specified in a FIPS or adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS (e.g., FIPS PUB 140-2).

[34] RSA™ was the first system that fitted the requirements of public-key cryptography and is the combined first letters of the last names of the collaborating creators of the RSA™ public-key system: R. L. **R**ivest, A. **S**hamir, and L. M. **A**dleman.

[35] An elliptic curve is not an ellipse. It is a set of solutions to a cubic polynomial in two variables, usually written in the form $y^2 = x^3 + Ax^2 + Bx + C$. If x ranges over all real numbers, such equations define curves that come in one or two pieces. Number theorists are interested in rational solutions for which the values of x and y can be written as fractions. An elliptic curve is *modular* if every rational solution can be found with "modular functions," which are advanced versions of the periodic functions found in geometry, such as sine and cosine.

[36] FIPS PUB 180-1, *Secure Hash Standard (SHS)*, specifies the SHA-1, which can be used to generate a condensed representation of a message called a message digest. When using the DSA to create digital signatures, messages are typically run through a cryptographic hash function, and the output of this function is what is actually signed. This output is called the message digest.

[37] The DSA is specified in FIPS PUB 186, *Digital Signature Standard (DSS)*.

[38] FIPS PUB 186-2, *Digital Signature Standard (DSS)*, provides cryptographic techniques based on public key cryptography for generating and verifying electronic signatures, which can be used to verify the origin and contents of a message. This standard is applicable to all federal departments and agencies for the protection of sensitive unclassified information that is not subject to Section 2315 of Title 10, U.S.C., or Section 3502(2) of Title 44, U.S.C.

DSTL DATA SHEET 17.1-6. STREAM CIPHERS

Stream ciphers encrypt individual characters (usually binary digits) of a plaintext message one at a time, using a symmetric key encryption transformation that varies with time.

H	(1) Are specified in approved national and international standards; (2) Have undergone extensive open peer review and has had no attacks that allow faster plaintext recovery than an exhaustive key search would allow; (3) Have no error propagation;[39] (4) Have symmetric-key strength appropriate for the security level of the data to be protected; and (5) Are secure against known-plaintext attacks.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Protecting civilian traffic on government, business, industry, and personal networks.
Affordability Issues	Competitive, stream encryption COTS products that have strong cryptographic functionality are appearing in the open market at little or no additional cost. However, the cost of security indoctrination and additional staff to manage and maintain secure cryptographic functionality for large complex systems is a significant cost issue.

BACKGROUND

Stream ciphers are generally faster than block ciphers in hardware and have less complex hardwire circuitry.[40] All stream ciphers have symmetric keys. The output of the keystream generator is a function of the key. Two basic types of stream ciphers are

1. *Synchronous* stream ciphers
2. *Self-synchronizing* or *asynchronous* stream ciphers.

A synchronous stream cipher is one in which the sender and receiver must be synchronized—using the same key and operating system at the same position (state) within that key—to allow for proper decryption. If synchronization is lost because ciphertext digits are inserted or deleted during transmission, the decryption fails and can only be restored through additional resynchronization techniques. These resynchronization techniques include reinitialization, placing special markers at regular intervals in the ciphertext, or, if the plaintext contains enough redundancy, trying all possible keystream offsets.[41]

A self-synchronizing or asynchronous stream cipher is one in which the keystream is generated as a function of the key and a fixed number of previous ciphertext digits.

> *Self-synchronization is possible if ciphertext digits are deleted or inserted because the decryption mapping depends only on a fixed number of preceding ciphertext characters. Such ciphers are capable of reestablishing proper decryption automatically after loss of synchronization, with only a fixed number of plaintext characters unrecoverable.*[42]

[39] No or zero error propagation means that a ciphertext digit that is modified (but not deleted) during transmission does not affect the decryption of other ciphertext digits.

[40] Alfred J. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, New York, 1997, pp. 191–192.

[41] Alfred J. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, New York, 1997, pp. 193–195.

[42] Alfred J. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, New York, 1997, p. 195.

Most well-designed stream ciphers have some form of nonce[43] or initialization vector, so that multiple messages can be sent with the same key.

A keystream generator, sometimes called a running-key generator, outputs a stream of bits the same size as the plaintext. At the encryption end, this running-key generator keystream is XORed[44] with the stream of plaintext bits to produce the stream of ciphertext bits. At the decryption end, the ciphertext bits are XORed with an identical keystream to recover the plaintext bits.[45]

Stream ciphers generally use fewer lines of code than block ciphers. RC4,[46] the most common stream cipher, is probably at least twice as fast as the fastest block cipher. RC4 can be written in perhaps 30 lines of code. The Software-optimized Encryption Algorithm (SEAL) and RC4 are binary additive stream ciphers specifically designed for fast software implementation and require a comparatively small number of lines of code.

A stream cipher can be viewed as a generalization of a one-time pad, where provable security is traded for practicality. While a one-time pad is provably secure, the key must be the same length as the plaintext, and the key cannot be reused, making it impractical for most applications. A stream cipher, on the other hand, effectively stretches a short secret key into a long pseudo-random keystream. The keystream is then used like the key in a one-time pad. To encrypt data, the stream cipher algorithm generates a keystream based on the key. The keystream can be as big as required to cover the plaintext of each message or packet. The algorithm XORs the plaintext with the pad. The stream cipher can generate this keystream on the fly, as needed. The Secure Socket Layers (SSLs) for secure connections on the Web uses the RC4 stream cipher because speed is extremely important and each connection can have a new key. Virtually all Web browsers and servers include RC4.

If a stream cipher is required, either a dedicated stream cipher or a mode of a block cipher can be chosen. Any block cipher can be transformed into a stream cipher using known modes of operation of the block cipher; it would work equally well in SSL, using counter CTR mode if a stream cipher is essential. In practice, there should be very few performance differences. In some cases, stream ciphers are a mandatory requirement for telecommunications applications and applications when buffering is limited or when characters must be individually processed as they are received. They have limited or no error propagation and are especially well suited to warfighter use in situations where transmission errors are highly probable.

.

[43] A nonce is a non-repeating value, such as a counter, used in key management protocols to thwart replay and other types of attack.

[44] XOR is the bit-by-bit modulo-2 addition of two binary vectors of equal length. In other words, the "Exclusive-OR" function is [binary] addition without carry. The XOR symbol is $\oplus$.

[45] Bruce Schneier, *Applied Cryptography, 2nd Edition*, John Wiley & Sons, Inc., New York, 1996, p. 197.

[46] Ron's code 4; named for its creator, Ron Rivest. RC4 is proprietary.

DSTL DATA SHEET 17.1-7. QUANTUM CRYPTOGRAPHY

Quantum cryptography is a form of cryptography that exploits quantum theory, in particular the *uncertainty principle*[47]—which states that it is impossible to measure all aspects of an object with absolute certainty.

Technology Parameter(s)	(1) Has protocols, operating systems, and application software that implement the quantum cryptographic functionality and that have undergone extensive open peer review, with no feasible attacks found; (2) Has real-time quantum encryption key generation and distribution; (3) Has optical fiber links > 50 km; and (4) Has the ability to penetrate the earth's atmosphere to space vehicles.
Critical Materials	None identified**.**
Unique Test, Production, Inspection Equipment	None identified**.**
Unique Software	Operating systems and application software implementing quantum cryptographic functionality and related techniques and software during the development, production, and operational life cycle so that the information systems match and maintain the required Common Criteria[48] EAL protection profile. Unique, empirically validated SE&I protocols, user system interface, algorithms, and key generators that have zero defects. Cryptographic module security that complies with the provisions of FIPS PUB 140-2, *Security of Cryptographic Modules* and the requirements of the NSA and is consistent with the appropriate ANSI standards for cryptography.
Major Commercial Applications	Key management for financial services system transactions. However, the near-term drivers that will be most important are the USG-funded satellite control and information security system applications.
Affordability Issues	Customizing quantum cryptography applications and features and the extensive SE&I experience, related techniques, and software during the development, production, and operational life cycle of quantum products are likely to be significant cost issues.

BACKGROUND

Charles H. Bennett, a fellow at IBM's Thomas J. Watson Research Center, and Gilles Brassard, a researcher at the University of Montreal in Canada, first devised quantum cryptography in 1984 as a part of their study of the relationship between physics and information. They were not searching for a new cryptographic method but simply applying some of the basic principles of quantum mechanics to real-world uses. What they discovered was that quantum mechanics is ideally suited for cryptography because of the one-wayness of photons.[49] In 1989, Bennett and his IBM colleagues built the first working quantum cryptographic prototypes, which sent photons a distance of 30 cm through the air of a laboratory. Most observers expect quantum cryptography to be the first practical application for quantum communications.

[47] The Heisenberg Uncertainty Principle. Given a particle has momentum, p, and a position, x in a quantum mechanical world I would not be able to measure p and x precisely. There is an uncertainty associated with each measurement (e.g., there is some dp and dx that I can never get rid of even in a perfect experiment). This is because whenever a measurement is taken, it must disturb the system. (For me to know something is there, I must bump into it.) The size of the uncertainties is not independent. It is roughly related by (uncertainty in p, dp) × (uncertainty in position, dx) is larger than h (= Planck's constant). The preceding is a statement of the Heisenberg Uncertainty Principle. So, for example, if I measure x exactly, the uncertainty in p, dp, must be infinite to keep the product constant.

[48] The *Common Criteria* is also ISO 15408.

[49] Edmund X. DeJesus, Quantum Leap, *Information Security*, August 2001, p. 72.

Quantum cryptography has now reached the point that it is no longer just a scientific investigation. It is clearly beginning to enter the technology phase, with at least three countries producing commercial quantum cryptography products that are, or soon will be, on the market. However, many issues are still in the scientific investigation phase.

Present applications of quantum cryptography are intended as a communication-encryption technology, not a storage-encryption technology. Quantum cryptography offers some potentially enormous communication-encryption advantages over conventional cryptosystems and may also be the only way to secure communications against the power of quantum computers.[50] Quantum cryptography guarantees the secure exchange of a random series of bits, which can then be used as the basis for a one-time pad cipher.[51]

With quantum methods, if the keys are used as one-time pads, complete security is assured. It is easy to use the collapse of quantum superpositions to generate truly random keys. This eliminates one of the major drawbacks of using one-time pads. In addition, the ability to detect the presence of an eavesdropper is a huge advantage over conventional methods.

Most of the current quantum cryptography systems are relatively simple. The sender randomly polarizes a stream of photons and transmits them to the recipient, who has special receiving equipment that can count and determine the polarization of individual photons on arrival. Once the recipient has enough photons and has determined their polarization, he/she can then tell the sender which photons he/she received. With that information, the sender can encrypt a message and send it over conventional media. In addition to polarization-based schemes, other quantum cryptographic systems have been devised to exploit different physical properties, but none of these have moved beyond the laboratory stage.

Conventional cryptography will be needed for many years and probably will never be completely replaced by quantum cryptography. Quantum cryptography provides for data confidentiality but does not provide message integrity or digital signatures (i.e., the message is secure assuming the laws of quantum mechanics as they are presently understood are true). However, without conventional cryptography, the identity of the originator is not known if the message is corrupted. As long as conventional cryptography is needed to develop a truly secure key management system, the attacker would still only have to break the conventional system to break the key management system.

Applied physicists at Stanford University have produced the first device that can create a beam of light with a steady stream of evenly spaced photons.[52] The successful creation of a *"single-photon turnstile device"* was first reported in the 11 February 1999 issue of *Nature*. This is a significant discovery because there are microscopic fluctuations imperceptible to the naked eye in ordinary light. These microscopic fluctuations are a major source of noise that has limited the development of a set of cutting-edge applications, collectively called *quantum information technology*. This term includes novel methods of computation and encryption that could ultimately be incorporated in mainstream computer and telecommunications devices. The noise caused by the irregular flow of photons has kept transmission rates in quantum cryptography systems down to a few thousand bits of information per second. This is very slow compared with the current optical communications rates, which are billions to trillions of bits per second. By contrast, the new turnstile device can only produce a stream of a million to 10 million photons per second, but an improved version is predicted that has the capability of increasing the transmission rate 200-fold.

[50] Paul E. Black, D. Richard Kuhn, and Carl J. Williams, "Quantum Computing and Communications," 2003, In *Advances in Computers,* Marvin Zelkowitx (Ed.), Vol. 56, Academic Press, 2002, pp. 189–244.

[51] Simon Singh, *The Code Book: The Evolution of Secrecy From Mary Queen of Scots to Quantum Cryptography*, Doubleday, New York, 1999, p. 321.

[52] Stanford, California, *Business Wire*, 12 February 1999. The single-photon turnstile device was created by a research team headed by Yoshihisa Yamamoto, professor of applied physics and electrical engineering at Stanford University. Team members included doctoral student Juangsang Kim, post-doctoral student Oliver Benson, and Hirofumi Kan Kan from Hamamatsu Photonics, Inc. in Japan. Physicists think of a beam of light as consisting of countless individual particles, known as photons, which exhibit wave-like properties.

SECTION 17.2 – CRYPTOGRAPHIC PROTOCOLS AND TECHNIQUES

Highlights

- Most of the *high-speed encryption* (HSE) investigation, research, and development is a search for solutions for data rates in the 1 to 10 Gbits-per-second range and is addressing a variety of challenges (e.g., how an originator authenticates in nanoseconds and how packet inspection firewall features can operate at high speeds[53].) The current front-end HSE work is concentrating on developing asynchronous transfer mode (ATM)[54] technologies for even higher rates. Old approaches to data security and integrity and authentication and access control are not fast enough to cope with the new high-speed, broadband networks.
- Secret sharing is important when a secret needs to be distributed over a set of ***n*** entities so that only authorized subsets of the entities can recover the secret.
- *Zero-knowledge proofs* (ZNPs) allow a prover to demonstrate knowledge of a secret while revealing no information of use to the verifier in conveying this demonstration of knowledge to others, beyond what the verifier was able to deduce before the protocol run.
- Perhaps the most critical issue concerning *key management* is the number of single points of failure. Certain management and user operations are required in any key management system. Even if human system interfaces are held to an absolute minimum, human frailty constitutes the biggest vulnerability. Every required human operation introduces several potential *modes of failure*. This technology is closely related to the DKG technology, which presents almost identical vulnerabilities.
- *Digital Data Steganography* is that branch of cryptology that attempts to obscure the existence of data through the use of subliminal channels. Cleartext or ciphertext can be randomly embedded in the quantization noise of image files or other data, without increasing the size of the host file.

OVERVIEW

This section outlines those identified cryptographic protocols and techniques that are being investigated and developed worldwide and have the potential to enhance or degrade future U.S. military capabilities significantly. It includes cryptographic protocols and techniques in basic research, associated applied research, and advanced technology development stages that are largely associated with cryptographic functionality in secure information processing systems.[55] These cryptographic protocols and techniques are associated with the more complex cryptographic applications, features, and functions.

Cryptographic protocols are discrete sets of standard conventions, policies, and procedures for each type of cryptography and are promulgated by duly constituted national and international standards bodies. These protocols govern the secure storage, handling, and communication of ciphertext, cryptographic keys, and related data.

Cryptographic techniques are the discrete, specified, and detailed sets of technical methods for implementing the standard conventions, policies, and procedures governing the secure storage, handling, and communication of ciphertext, cryptographic keys, and related data for each type of cryptography.

[53] Nicholas Cravotta, "Accelerating High-Speed Encryption: One Bottleneck After Another," *EDN Europe*, September 2001, p. 37.

[54] A broad-bandwidth, low delay, packet-like (cell relay) switching and multiplexing technique.

[55] Information processing systems is a collective term that covers both computers and telecommunications.

Cryptologic scientific investigations and developing cryptographic protocols and techniques are closely related to those in information technology (Section 10). Information security modules, components, and systems must be tightly integrated with, if not an integral component or module of, information processing hardware and software architecture. Many applications now incorporate high-performance features and metaprocessing (or grid)[56] techniques that are shortening the cryptanalytic time required for an exhaustive key search. This makes the information processing technologies (Section 10.3) closely related to this information security section, especially HPC technologies. The length of time required for cryptanalyses is a function of both

- Knowledge in the field of mathematics
- The state of the art in HPC.

The progress in mathematical knowledge may be characterized as slow, so the time required for cryptanalytic procedures and techniques is largely dependent on the state of the art in HPC because processing power is still increasing rapidly.[57] Processing power determines the time required to perform an exhaustive key search, which, in turn, governs the life cycle of most algorithms and key lengths.

Information Security technologies are also closely related to the TT&C encryption and decryption technologies for military systems. The commanding uplinks and mission data downlinks for some civilian and all military satellites (e.g., the GPS) are protected by encryption to maintain positive control of the satellite systems and prevent mission data interception, intrusion, and spoofing.

It can be argued that key recovery system failure mode and effects analyses and secret sharing schemes are logical subsets of key management; however, they covered in separate data sheets (17.2-5 and 17.2-5) to provide finer identification and specification and to avoid potential ambiguity in the threshold specifications.

BACKGROUND

Cryptology changed when Claude Shannon, a mathematician at Bell Laboratories, showed how the once-vague notion of information could be defined and quantified with absolute precision. He showed that every mode of communication could be encoded in the universal language of *b*inary dig*its*, or *bits*—a term that was first used in 1948 and from which the entire science of information theory grew. This discovery, in turn, made possible the use of von Newman's deterministic computers for both cryptography and cryptanalysis.

Joint Publication *1-02*, *Department of Defense Dictionary of Military and Associated Terms* contains no definition for cryptographic protocols or for cryptographic techniques; however, it defines cryptology as follows:

> *Cryptology is the science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence*.

NIST is responsible developing cryptographic standards and guidelines to protect the SBU information of federal government departments and agencies.[58] The NIST cryptographic standards, some of which are mentioned in this section, are also widely used by defense industry and many other nongovernmental activities, including businesses and the financial services industry. Many of the definitions and much of the cryptographic information in this section are drawn, at least in part, from NIST publications.

[56] Ian Foster of the Argonne National Laboratory originally coined the term "*grid computing*" in the 1990s. He proposed a grid to coordinate computing resources that are not centrally controlled, rely on open standards, and provide more processing power and reliability than stand-alone machines. Other names for various permutations and variations are *metaprocessing, Internet computing,* and *cycle scavenging*.

[57] In 1965, Gordon Moore made the prediction that processor speed would double every 18 months. In 1968, Moore co-founded Intel Corporation. The increase in commodity processor speeds is still obeying *Moore's Law*, doubling about every 18 months and is generally predicted by most of today's authorities to continue to obey this law for about 10 more years. (See *Electronics*, 19 April 1965, p. 114).

[58] FIPS PUBS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

The cryptographic protocols and techniques used in cryptographic systems are just as important as the algorithms and key lengths chosen to secure the information. The mathematics and hard problems chosen as the basis for cryptographic algorithms are almost never the cause of a security breach. Human frailty is the biggest single cause of security breaches. The next biggest causes are weak cryptographic protocols and techniques, buggy software, and poorly integrated cryptographic applications and functionality.

LIST OF DSTL TECHNOLOGY DATA SHEETS
17.2. CRYPTOGRAPHIC PROTOCOLS AND TECHNIQUES

DSTL DATA SHEET 17.2-1. ELECTRONIC MONEY TRANSFER

Electronic money transfer technology includes products such as credit cards, electronic checks (e-checks), electronic wallets (e-wallets), and prepaid credit cards for shopping and person-to-person money transfer.

Technology Parameter(s)	Interoperable secure electronic cash (e-cash) payment software in smart-card-based systems with (1) A secure multi-function card;[59] (2) An imbedded 16-bit on-board processor; (3) 128 Kbytes of imbedded data storage; and (4) An on-board crypto module[60] that supports a 128-bit AES symmetric key[61] or two 1,024-bit RSA[62] or Digital Signature Algorithm/Diffie-Hellman (DSA/DH) asymmetric keys [63] or two 161-bit Elliptic Curve Digital Signature Algorithm/Elliptic Curve Diffie-Hellman (ECDSA/ECDH) keys and an ANSI-approved hash function or SHA-1 hash [64] that are USG Smart Card Interoperability Specification[65] compliant. Tamper-resistant cards that are ISO 7810 and 7816 or 14443 compliant, having associated secure card fabrication and initialization equipment.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Most application software for COTS secure e-cash transfer systems is proprietary. The operating systems are usually either proprietary commercial operating systems, such as IBM's S390/MVS (Multiple Virtual Storage), Mondex's Multos, Sun Mircosystem's Java Card™, or the Mac O/S, or quasi-open systems, such as Compaq Open VMS and Linux, which are used to provide cross-platform multivendor database synchronization.
Major Commercial Applications	The financial services industry has a full spectrum of vendors, although USG and commercial smart card markets are limited in number. Foreign commercial use is widespread, especially in Europe, by various financial, telephone, and cellular service industries, which have been the drivers. The current commercial base is in industries and vendors in transportation, banking and financial services, manufacturing and distribution, education, and health care.
Affordability Issues	E-cash cards are the inexpensive components or system segments of electronic money (e-money) transfer systems. The cost issues are largely in the other system segments and system utilization costs associated with risk and convenience factors.

[59] *Identification Cards-Integrated Circuit (s) Cards With Contacts: Additional Interindustry Commands and Security Attributes*, BS ISO/IEC 7816-4 through -9 or contactless cards that are ISO/IEC 14443 Type B, Contactless Memory.

[60] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* (X9.66), and CMVP (Cryptographic Module Validation Program) compliant. (For information on the CMVP, see http://csrc.nist.gov/cryptval/).

[61] FIPS PUB 197, *Advanced Encryption Standard (AES)*; ANSI X9.91.

[62] ANSI X9.44, *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: Management of Symmetric Keys Using RSA*, and FIPS PUB 197, *Advanced Encryption Standard* (AES) compliant.

[63] ANSI X9.30-1997, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry*, *Part 1*, *The Digital Signature Algorithm (DSA)*; American National Standards Institute, American Bankers Association; and, ANSI X9.30-1997, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry*, *Part 2*, *The Secure Hash Algorithm (SHA)*; American National Standards Institute, American Bankers Association; X9.42-2003, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*; and ANSI X9.62-1999, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (EDCSA)* compliant.

[64] ANSI X9.31-1998, *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry*, *The RSA Signature Algorithm (RSA)*; American National Standards Institute, American Bankers Association, and FIPS PUB 180-2 *Secure Hash Standard (2002)* and 186-2, *Digital Signature Standard*, 27 January 2000, compliant. Two asymmetric keys are required: one to provide signatures and the other for (symmetric) key establishment. SHA-1 is a hash function and is not keyed.

[65] Government Smart Card Interoperability Specification (GSC-IS), Vol. 2.1, 16 July 2003, NIST (http://smartcard.nist.gov).

BACKGROUND

Public-key cryptography and digital signatures (both blind and non-blind signatures) make e-money possible. Banks and customers have public-key encryption keys, which function in pairs: a private key known only to the owner and a public key made available to everyone. Whatever the private key encrypts, the public key can decrypt, and vice versa. Banks and customers use their keys to encrypt (for security) and sign (for identification) blocks of digital data that represent money orders. A bank “signs” money orders using its private key. Customers and merchants verify the signed money orders using the bank’s widely published public key. Customers sign deposits and withdrawals using their private key, and the bank uses the customer’s public key to verify the signed deposits and withdrawals.

In general, the two distinct types of e-money are identified e-money and anonymous e-money (also known as digital cash). Identified e-money contains information revealing the identity of the person who originally withdrew the money from the bank. Also, in much the same manner as credit cards, identified e-money enables the bank to track the money as it moves through the economy. Anonymous e-money works just like currency. Once anonymous e-money is withdrawn from an account, it can be spent or given away without leaving a transaction trail. Anonymous e-money is created by using blind signatures[66] rather than non-blind signatures.

Online e-money systems prevent double spending by requiring merchants to contact the bank’s computer with every sale. The bank computer maintains a database of all the spent pieces of e-money and can easily indicate to the merchant if a given piece of e-money is still spendable. If the bank computer says the e-money has already been spent, the merchant refuses the sale. This is similar to the way merchants currently verify credit cards at the point of sale.

Offline e-money systems detect double spending in several different ways. One method is to create a special smart card containing a tamper-proof chip called an Observer (in some systems). The Observer chip keeps a mini database of all the pieces of e-money spent by that smart card. If the owner of the smart card attempts to copy some e-money and spend it twice, the imbedded Observer chip would detect the attempt and would not allow the transaction. Since the Observer chip is tamper-proof, the owner cannot erase the mini database without permanently damaging the smart card. Another other way offline e-money systems handle double spending is to structure the e-money and cryptographic protocols to reveal the identity of the double spender by the time the piece of e-money makes it back to the bank. If users of the offline e-money know they will get caught, the incidence of double spending will be minimized (in theory). The advantage of these kinds of offline systems is that they do not require special tamper-proof chips. The entire system can be written in software and can run on ordinary PCs or low-cost smart cards.

Constructing this kind of offline system for identified e-money is easy. Offline identified e-money systems can track the complete path the e-money made through the economy. The identified e-money “grows” each time it is spent. The particulars of each transaction are appended to the piece of e-money and travel with it as it moves from person to person, merchant to vender. When the e-money is finally deposited, the bank checks its database to see if the piece of e-money was double spent. If the e-money was copied and spent more than once, it will eventually appear twice in the “spent” database. The bank uses the transaction trails to identify the double spender.

Offline anonymous e-money (without an Observer chip) also grows with each transaction, but the accumulated information is of a different nature. The result is the same however. When the anonymous e-money reaches the bank, the bank will be able to examine its database and determine if the e-money was double spent. The information accumulated along the way will identify the double spender.

The big difference between offline anonymous e-money and offline identified e-money is that the information accumulated with anonymous e-money will only reveal the transaction-trail if the e-money is double spent. If the anonymous e-money is not double spent, the bank cannot determine the identity of the original spender nor can it reconstruct the path the e-money took through the economy. With identified e-money, both offline or online, the bank can always reconstruct the path that the e-money took through the economy. The bank will know what everyone bought, where he/she bought it, when she/she bought it, and how much he/she paid..

[66] To understand the advanced protocols for blind signatures, see Bruce Schneier, *Applied Cryptograph: Protocols, Algorithms, and Source Code in C*, Second Edition, John Wiley & Sons, Inc., 1996, p. 112.

DSTL DATA SHEET 17.2-2. HIGH-SPEED ENCRYPTION (HSE)

HSE is a technology that could minimize the performance impact of secure communications services in high-speed [Optical Carrier (OC)-12 (622 Mbit/sec) and above] networks.

Technology Parameter(s)	Encryption for (1) High-speed networks [OC-12 (622 Mbit/sec) and above] and (2) ATM networks.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Operating systems and application software implementing quantum cryptographic functionality, related techniques, and software during the development, production, and operational life cycle so that the information systems match and maintain the required Common Criteria[67] EAL protection profile of the cryptosystem. The unique, empirically validated SE&I, protocols, user system interface, algorithms, and key generators that have zero defects. Cryptographic module security that complies with the provisions of FIPS PUB 140-2, *Security of Cryptographic Modules* and NSA requirements and is consistent with the appropriate ANSI standards for cryptography.
Major Commercial Applications	HSE is expected to become a dual-use technology because of the commercial requirement to increase the speed and security of communications.[68] The financial services community and e-commerce interests are now demanding more bandwidth and more secure telecommunications for electronic funds transfer applications and various e-commerce applications.
Affordability Issues	None identified.

BACKGROUND

Most HSE investigation, research, and development is searching for solutions for data rates in the 1 to 10 Gbits per second range and is addressing a variety of challenges, such as how an originator authenticates in nanoseconds and how packet inspection firewall features can operate at high speeds.[69] The current front-end HSE work is concentrating on developing ATM technologies for even higher rates. Old approaches to data security and integrity and to authentication and access control are not fast enough to cope with the new high-speed, broadband networks.

HSE may be application ready soon.

[67] The *Common Criteria* is also ISO 15408.

[68] Cylink already has 45 Mbit/sec ATM encryption products on the market.

[69] Nicholas Cravotta, "Accelerating High-Speed Encryption: One Bottleneck After Another," *EDN Europe*, September 2001, p. 37.

DSTL DATA SHEET 17.2-3. KEY MANAGEMENT

Key management is the generation, storage, secure distribution, and application of keying material during the lifetime of the key(s) in accordance with a security policy.[70]

Technology Parameter(s)	Perform the required failure mode and effects analysis to identify and fix potentially vulnerable techniques, functionalities, and protocols (most of which require human intervention) and introduce points of failure through (1) New scientific investigation and research results that have the potential to enhance or degrade key management capabilities significantly; (2) Application of early results from basic and applied scientific investigation and R&D in key management schemes; (3) Fixing vulnerabilities discovered during key management system research findings in failure mode and effects analyses; and (4) Application of all new techniques, protocols, and procedures that have the potential to enhance or degraded existing key management capabilities significantly for U.S. Class A or Class B cryptographic systems.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Failure mode and effects analyses models; software required to investigate, discover, and implement new scientific and technological discoveries that could have the potential to enhance or degrade significantly future U.S. key management capabilities; software that supports empirical security SE&I methodology and procedures.
Major Commercial Applications	The information security industry supplies key management commercial applications and service to the financial services industry, telecommunications industry, legal and medical services, and developers of a wide variety of e-commerce applications, services, and personal privacy products. The threats from independent hackers and from nation states, rogue states, terrorists, and international criminals drive this technology.
Affordability Issues	The expensive and time-consuming basic research required to produce key management system discoveries and create the technologies with which to produce military products and perform exhaustive failure mode and effects analyses is most likely to be financed by nation states or niche universities. Military requirements, not affordability, are the principal military acquisition issues for this technology. The cost of additional staff, processor power, and memory capacity to operate, manage, and maintain the key management cryptographic functionality for large complex systems can be a significant cost issue. Most of this functionality can be automated. However, there is still a potentially expensive requirement of recruiting and retaining technically qualified, trustworthy, responsible personnel to operate and manage the system and support the required end-user training, standardization, and T&E programs required for optimum protocol security.

BACKGROUND

One of the principal functions of the key management system is the recovery function for a cryptographic system key fault. *Key fault* means that there has been the loss of, or damage to, a key. *Key recovery* is a generic term for the systematic protection of encryption keys to prevent their loss (see DSTL Data Sheet 17.2-4). *Key life* extends from key generation through use, protection, and key destruction.

[70] TR-1 – 1999, *Technical Guide for ABA/ASC X9 Standards Definitions, Acronyms and Symbols* (ABA = American Bankers Association; ASC = Accredited Standards Committee).

DSTL DATA SHEET 17.2-4. KEY RECOVERY SYSTEM FAILURE MODE AND EFFECTS ANALYSES

Key recovery is a generic term for the systematic protection of encryption keys to prevent their loss. It is also a collective term that applies to different techniques and schemes that provide users the ability to recover plaintext from encrypted text, files, and data in case there is a *key fault* (i.e., the key has been lost or damaged).[71]

Technology Parameter(s)	(1) Significantly increased reliability and security of recovery systems with some number of all those TTPs holding portions of the key; (2) Multi-TTP schemes; (3) Reproducible results that significantly enhance or degrade current U.S. military multi-TTP key recovery systems; and (4) Significantly enhance or degrade existing multi-TTP key recovery capabilities for USG Class A or Class B cryptographic systems.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Failure mode and effects analyses models.
Major Commercial Applications	The information security industry supplies key management commercial applications and service to the financial services industry, telecommunications industry, legal and medical services, and developers of a wide variety of e-commerce applications, services, and personal privacy products. The threats from independent hackers and from nation states, rogue states, terrorists, and international criminals drive this technology.
Affordability Issues	The expensive and time-consuming basic research required to produce trusted key recovery feature discoveries and create the technologies with which to produce militarily critical products with the critical technology parameters specified in the first row of this data sheet table and perform the supporting exhaustive failure mode and effects analyses is most likely to be financed by nation states or niche universities. Military requirements, not affordability, are the principal military acquisition issues for this technology. Affordable, competitive, new general-purpose key management, including key recovery functionality, COTS products and services suitable for military applications are appearing in open markets and include strong cryptographic functionality at little or no additional cost. The cost of additional staff, processor power, and memory capacity to operate, manage, and maintain the key management and recovery cryptographic functionality for large complex systems can be a significant cost issue. Most of this functionality can be automated. However, there is still a potentially expensive requirement of recruiting and retaining technically qualified, trustworthy, responsible personnel to operate and manage the system and support the required end-user training, standardization, and T&E programs required for optimum protocol security.

BACKGROUND

Key escrow and recovery archiving systems are developing rapidly. However, the protocols for these systems do not have the proven integrity, predictability, and trust of the traditional protocols that involve only the sender and the recipient to guarantee the security of cryptographic keys. The goal of *key recovery* scientific investigation and R&D is to prove the integrity, predictability, and trust of multiple user key escrow and recovery archiving systems so that these systems will engender the same trust of the traditional legacy protocols (protocols that involve only the classic sender and the recipient in legacy systems to guarantee the security of cryptographic keys).

[71] Recovery of Encrypted Data, *ITL Bulletin*, April 2002, p. 3 [ITL = Information Technology Laboratory (NIST)].

A general key escrow system is equivalent to (can be reduced to) a system secure against a *chosen-ciphertext attack*,[72] and an escrow system (with certain accountability features) equivalent to a *non-malleable*[73] cryptographic system.

Key life extends from key generation through use, protection, and key destruction. Cryptographic *key life expectancy* is a function of the state of the art in high-speed computing and the state of the art in cryptanalysis. For example, the discovery of an improved Number Field Sieve or a faster, more natural factorization algorithm may also affect the asymmetric key life cycle. Cryptographic strength and key life cycles are among the most critical technical issues in cryptology.

To provide an overview of the complexities in the key recovery aspect of key management systems, four examples of conventional key recovery approaches are provided:[74]

1. *Key Escrow* was introduced with the Clipper Chip and Escrowed Encryption Standard (EES). A sender or a ciphertext producer escrows the key (e.g., session keys) to one or more key escrow agents. When the key needs to be recovered, the receiver or authorized *jurisdiction* requests the escrowed keys from the escrow agents. The jurisdiction is a government or company to which the receiver is subordinated.[75]
2. In a TTP *(Trusted Third Party)*[76] system, a sender obtains a key from the TTP (e.g., key distribution center). To recover the key, a receiver or jurisdiction requests the distributed key from the TTP.
3. *Commercial Key Backup*[77] services are provided by commercial organizations such as AT&T Crypto-Backup. A sender symmetrically encrypts some information using a session-key, asymmetrically encrypts the session-key using his public-key, and maintains the results. In addition, the sender's private-key should be saved at a backup agent. On recovering the key, a receiver or jurisdiction requests the stored private-key from the agent.
4. In a *Key Encapsulation* system, a sender generates the Key Recovery Information (KRI) by means of a symmetric encryption of information using a session-key and then asymmetrically encrypts the session-key using the public-key of the Key Recovery Agent (KRA). The KRI is encapsulated into ciphertext messages or files. On recovering the session key, a receiver or jurisdiction requests recovery of the session-key from the KRA. The key encapsulation is a *distributed key recovery* approach (i.e., each sender and receiver generates and stores his own KRI). The KRA does not store any KRI as long as a receiver does not request a key recovery service from the KRA. The approach reduces a bottleneck, and the user's privacy might be ensured since each user would have the authority of recovery.

In an effort to overcome some of the problems discovered in the conventional key recovery approaches, the n-Way Key Recovery System was developed. This system conforms to NIST's FIPS PUB 171, *Key Management Using ANSI X9.17*, which has become a de facto international standard for key recovery and CC 2.0.[78]

[72] A *chosen-plaintext attack* is one where the adversary chooses plaintext and is then given corresponding ciphertext. Subsequently, the adversary uses any information deduced to recover plaintext corresponding to previously unseen ciphertext.

[73] A public-key encryption system is said to be *non-malleable* if given a ciphertext, it is *computationally infeasible* to generate a different ciphertext such that the respective plaintexts are related in a known manner. *Computationally infeasible* means that it is judged infeasible to perform an exhaustive key search and recover the plaintext, with the present state of the art in mathematics and processor power, in time to have any practical utility.

[74] D. Denning and K. Dennis, "A Taxonomy for Key Escrow Encryption System," *Communications of the ACM,* Vol. 39, No. 3, March 1996, pp. 34–40.

[75] Shin-Young Lim et al., "Specification and Analysis of n-Way Key Recovery System by Extended Cryptographic Timed Petri Net," *Journal of Systems and Software,* Vol. 58, 2001, pp. 93–106.

[76] ANSI X9.17 [the Financial Institution Key Management (Wholesale) standard].

[77] Shin-Young Lim et al., "Specification and Analysis of n-Way Key Recovery System by Extended Cryptographic Timed Petri Net," *Journal of Systems and Software,* Vol. 58, 2001, pp. 93–106.

[78] *Security Evaluation* (CC Version 2.1), which is identical to *International Standard ISO/IEC 15408.*

The n-Way Key Recovery System[79] was developed by Shin-Young Lim, Jeong-Ho-Ko, Eun-Ah Jun, and Gang-Soo Lee in 2001. This variation is gaining some considerable interest in the cryptographic community. The developers of the n-Way Key Recovery System also proposed a new modeling and analysis model, an *Extended Cryptographic Timed Petri Net* (ECTPN), for formal modeling and analysis of the n- Way Key Recovery System.

[79] Shin-Young Lim et al., “Specification and Analysis of n-Way Key Recovery System by Extended Cryptographic Timed Petri Net,” *Journal of Systems and Software,* Vol. 58, 2001, pp. 93–106.

DSTL DATA SHEET 17.2-5. SECRET SHARING SCHEMES

Secret sharing schemes, which are sometime called *threshold schemes*, allow a secret to be shared among a limited set of participants so that only qualified subsets of participants can recover the secret.[80]

Technology Parameter(s)	Proactive signature schemes[81] to ensure that the private key can never be assembled under accidental or unauthorized conditions in which it could be compromised.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Secret sharing models.
Major Commercial Applications	The information security industry supplies secret sharing features as functions of key recovery commercial applications and service to the financial services industry, telecommunications industry, legal and medical services, and developers of a wide variety of e-commerce applications, services, and personal privacy products. The financial services industry uses secret sharing schemes to protect master keys. CAs use secret sharing schemes to protect the root private key. Many commercial enterprises use secret sharing schemes for key recovery in case emergency access is required.
Affordability Issues	The expensive and time-consuming scientific investigations and basic R&D required to produce trusted key recovery features using secret sharing (or *secret splitting*)[82] schemes and to create trusted products is most likely to be financed by nation states or niche industries and universities. Affordable, competitive, new general-purpose key management, including key recovery functionality, COTS products and services suitable for military applications are appearing in open markets and include strong cryptographic functionality at little or no additional cost. The cost of additional staff, processor power, and memory capacity to operate, manage, and maintain the key management and recovery cryptographic functionality for large complex systems can be a significant cost issue. Most of this functionality can be automated. However, there is still a potentially expensive requirement of recruiting and retaining technically qualified, trustworthy, responsible personnel to operate and manage the system and support the required end-user training, standardization, and T&E programs required for optimum protocol security.

BACKGROUND

Secret sharing is a broad term that applies to many different techniques and schemes that provide users with the ability to recover plaintext from encrypted text, files, and data. It is important when a secret needs to be distributed over a set of *n* entities so that only authorized subsets of entities can recover the secret. This is a fairly new technique and is still moving rapidly. Dozens of secret sharing schemes have been proposed in the last 25 years. New visual secret sharing schemes have been proposed recently (2004).[83]

[80] A. De Bonis and A. De Santis, “Randomness in Secret Sharing and Visual Cryptography Schemes,” *Theoretical Computer Science*, Vol. 314, No. 3, 2004, pp. 351–374.

[81] Proactive signature techniques are important in Root or Bridge CA applications in PKIs.

[82] RSA name used for their new Nightingale™ product.

[83] Ching-Nung Yang, “New Visual Secret Sharing (VSS) Schemes Using Probabilistic Method,” *Pattern Recognition Letters*, Vol. 25, 2004, pp. 481–494.

The fundamental approach to secret sharing was devised independently by Shamir[84] and Blakley[85] in 1979 and is called the (***m, n***) scheme. A (***m, n***) threshold secret sharing scheme is a protocol between ***n***+1 players (including the dealer and ***n*** participants) in which the dealer distributes partial information (a shadow in the jargon) about a secret to ***n*** participants such that

- Any group of fewer than ***m*** participants cannot obtain any information about the secret
- Any group of at least ***m*** participants can compute the secret in polynomial time.[86]

At this time, secret sharing appears to be the best solution to many military and civilian business application key management and recovery problems. Secret sharing schemes are at the heart of some key management and recovery systems in which several participants in the access structure may hold portions of the key. The key must be shared in such a way that only authorized subsets can determine the key. This developing technology is moving rapidly.

The USG key escrow scheme[87] is also a form of secret sharing in which the Law Enforcement Access Field (LEAF) portion of a cryptographic key is divided between two agencies and then redivided within each agency—in effect, providing at least four-person control. Most commercial key recovery schemes also use some form of secret sharing.

RSA Laboratories developed an innovative form of secret sharing, which they call "*secret splitting*," that is engineered to improve the security and privacy of conventional servers for all types of sensitive data. The sensitive data are cryptographically distributed across two separate servers: the Nightingale server and any application server. The Nightingale system provides a way for two servers or other computing devices to use two parts of a shared secret—a cryptographic key—without revealing the value of the key itself. The key is then employed to decrypt the requested data. The data encryption process happens only once when using a split secret; therefore, the computationally intense process of scrambling the private data occurs only once.[88]

In a secret sharing scheme, a secret value is distributed into shares among the participants in a set ***P*** in such a way that only qualified subsets of ***P*** can reconstruct the secret from their shares.[89]

Lukac, Plataniotis, and Venetsanopoulos have proposed a new (2004) ***{k, n}***-secret sharing scheme for color images that also could be classified as a form of steganography. The proposed method encrypts the color image into ***n*** color shares. The secret information is recovered only if the ***k*** (or more) allowed shares are available for decryption. The proposed method uses the conventional ***{k, n}***-secret sharing strategy by operating at the bit-levels of the decomposed color image. Modifying the spatial arrangements of the binary components, the method produces color shares with varied spectral characteristics among the Red-Green-Blue (RGB) components and the spatial correlation between the neighboring color vectors. Since encryption is done in the decomposed binary domain, there is no obvious relationship in the RGB color domain between any two of the color shares or between the original color image and any of the ***n*** shares. This increases protection of the secret information. Inverse cryptographic processing of the shares must be realized in the decomposed binary domain, and the procedure reveals the original color image with perfect reconstruction. [90]

[84] A. Shamir, "How To Share a Secret," *Communications of the ACM,* 1979, Vol. 22, pp. 612–613.

[85] G. R. Blakley, *Safeguarding Cryptographic Keys,* In Proceedings of the National Computer Conference, 1979, pp. 313–317.

[86] Polytime code is ***polynomial-time (P)***: ***P*** is a so-called $\boldsymbol{n^2}$ *algorithm* for *solving* problems in which the processing time increases as the square of the data processed.

[87] FIPS PUB 185, *Escrowed Encryption Standard (EES).*

[88] Cameron Sturdevant, RSA Splits Keys to Lock Up Data, *eWEEKLABS*, 28 April 2003, p. 61.
Also see http://www.rsasecrity.com/press_asp?_id+2442&id=1034.

[89] Tan Xiaoqing and Wang Zuhiguo, "New Secret Sharing Scheme Based on Linear Code," *Applied Mathematics Journal*, Chinese University, Series B, Vol. 19, No. 2, 2004, pp. 160–166 (supplied by the British Library).

[90] Rastislav Lukac, Konstantinos N. Plataniotis, and Anastasios N. Venetsanopoulos, *A **{k, n}**-Secret Sharing Scheme for Color Images*, Computational Science – ICCS 2004: 4th International Conference, Kraków, Poland, June 6–9, 2004, pp. 72–79.

The new ***{k, n}*** secret sharing scheme introduced at the University of Toronto produces perfect reconstruction of the color inputs. The method cryptographically processes the color images, replacing the 79 bit components of the *A **{k, n}**-Secret Sharing Scheme for Color Images* with a block of bits for each of the ***n*** shares. By separately encrypting each bit plane of the decomposed color image, the method produces color shares with varied spectral and spatial characteristics. Since encryption is realized in the decomposed binary domain, the procedure increases protection against attacks performed in the RGB (red, blue, green) color domain. This makes the method attractive for secure transmission over untrusted public channels. The perfect reconstruction property allows the revelation of the original color image without visual impairments or color shifts.[91]

The Lukac, Plataniotis, and Venetsanopoulos secret sharing technique for cryptographic color image processing method operates in the decomposed bit-levels of the input color vectors to change both spatial and spectral correlation characteristics of the share outputs and produce random, color-noise-like images for secure transmission, and access. The decryption process satisfies the perfect reconstruction property and recovers the original color image by logically decrypting the decomposed bit vector-arrays of the color shares.

[91] Rastislav Lukac, Konstantinos N. Plataniotis, and Anastasios N. Venetsanopoulos, *A **{k, n}**-Secret Sharing Scheme for Color Images*, Computational Science – ICCS 2004: 4th International Conference, Kraków, Poland, June 6–9, 2004, pp. 72–79.

DSTL DATA SHEET 17.2-6. ZERO-KNOWLEDGE PROOFS (ZNPs)

Zero-knowledge proofs (ZNPs) are methods for proving knowledge of a secret without revealing any information about the secret.

Technology Parameter(s)	(1) Prove knowledge of a secret without revealing any knowledge of the secret; [92] (2) Prove identification; (3) Provide verification; Reproducible results that significantly enhance or degrade current U.S. military zero-knowledge proof schemes; and (4) Significantly enhance or degraded existing cryptographic capabilities for USG Class A and Class B cryptographic systems.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	ZNP models.
Major Commercial Applications	The ZNP characteristic of anonymity is an important part of some concepts for e-commerce transactions. For example, proof of certain generic authority or credit "credentials" might be provided for e-commerce without revealing identity by using ZNP systems. E-commerce transactions that protect privacy. Like all requirements for security on the Internet, the threats from independent hackers and from nation states, rogue states, terrorists, and international criminals drive this technology.
Affordability Issues	Not an issue at this time.

BACKGROUND

ZNPs allow a prover to demonstrate knowledge of a secret while revealing no information whatsoever of use to the verifier in conveying this demonstration of knowledge beyond what the verifier was able to deduce before the protocol run. Only a single bit of information has to be conveyed—namely, that the prover actually does know the secret. ZNP protocols provide trusted authentication mechanisms and anonymity. For example, one could prove U.S. citizenship without providing any other specific information such as name, address, sex, or exact age.

A protocol that is a proof of knowledge has the zero-knowledge property if it can be simulated in the following sense: there exists an expected polynomial-time algorithm (simulator) which can produce, upon input of the assertion(s) to be proven but without interacting with the real prover, transcripts indistinguishable from those resulting from interaction with the real prover. The zero-knowledge property implies that a prover executing the protocol, even when interacting with a malicious verifier, does not release any information about its secret knowledge other than that the particular assertion itself is true, not otherwise computable in polynomial time[93] from public information alone. Thus, participation does not increase the chances of subsequent impersonation.[94]

A protocol is computationally zero-knowledge if an observer restricted to probabilistic polynomial time tests cannot distinguish real from simulated transcripts. For perfect zero-knowledge, the probability distributions of the transcripts must be identical. By convention, when not further qualified, zero-knowledge means computational zero-knowledge. In the case of computational zero-knowledge, real and simulated transcripts are said to be polynomially

[92] For example, proving knowledge of a key without revealing anything about the key.

[93] The polynomial time or "polytime" code notation is P, a so-called $\boldsymbol{n^2}$ algorithm for ***solving*** problems in which the processing time increases as the square of the data processed.

[94] Alfred J. Menezes, Paul C. vanOrschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, New York, 1997, p. 407.

indistinguishable (indistinguishable using polynomial-time algorithms). Any information extracted by a verifier through interaction with a prover provides no advantage to the verifier within polynomial time.[95]

Interesting work has been done in statistical zero-knowledge protocols (e.g., statistical zero-knowledge protocols to prove statements, such as the work of Jan Camenisch and Markus Michels):

> *A committed number is a prime. A committed (or revealed) number is the product of two safe primes, i.e., primes p and q such that (p-1)/2 and (q-1)/2 are prime. A given integer has large multiplicative order modulo a composite number that consists of two safe prime factors. The main building blocks of these protocols are statistical zero-knowledge proofs of knowledge that are of independent interest. There has been proof of the correct computation of a modular addition, a modular multiplication, and a modular exponentiation, where all values including the modulus are committed to but not publicly known. Apart from the validity of the equations, no other information about the modulus (e.g., a generator whose order equals the modulus) or any other operand is exposed. These techniques can be generalized to prove that any multivariate modular polynomial equation is satisfied, where only commitments to the variables of the polynomial and to the modulus need to be known. This improves previous results, where the modulus is publicly known.*[96]

[95] Alfred J. Menezes, Paul C. vanOrschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, New York, 1997, p. 407.

[96] Jan Camenisch and Markus Michels, *Proving in Zero-Knowledge That a Number Is the Product of Two Safe Primes*, BRICS Department of Computer Science, University of Aarhus, Ny Munkegade, Denmark, 2004.

DSTL DATA SHEET 17.2-7. DIGITAL DATA STEGANOGRAPHY

Steganography is that branch of cryptology that attempts to obscure the existence of data through the use of subliminal channels. Cleartext or encrypted information can be randomly embedded in the quantization noise of digital images or other imprecise digital data files, without noticeably increasing the size of the host file.

Technology Parameter(s)	Meet the specified point on the applicable biometric scale at which the embedded covert data are below the detectable threshold for each type of digital data[97] (e.g., 2 bits of information per pixel in 8-bit image files for the human eye). At this rate, a picture file could carry a 5- to 10-percent randomly embedded information data set before it becomes visually or statistically detectable.[98]
Critical Materials	None identified**.**
Unique Test, Production, Inspection Equipment	High-performance computers specially designed to perform statistical tests to determine the detectability of disguised or hidden data during development, test, and evaluation of digital steganographic systems.
Unique Software	The digital image steganographic software security SE&I, user system interface, protocols, algorithms, and imbedding generators must have zero defects and comply with the applicable provisions of FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*.
Major Commercial Applications	Commercial application requirements and research are driving this technology: (1) personal and commercial steganographic applications are widely available for watermarking and imbedding covert data in images, video, audio, or text files for authentication and for copyright and patent protection; (2) research prototypes and proof-of-concept applications are the drivers for this technology; and (3) building on the current digital image steganography market, commercial uses for digital image steganography in the protection of intellectual property could be even wider. Copyrighted data could be watermarked with digital image steganography. Digital image forms of artwork should be especially easy to watermark to provide proof of ownership or origin, as would any other electronic data image products sold in e-commerce over the Internet.
Affordability Issues	Affordability should not be the principal acquisition issue for digital image steganographic products. Competitive new COTS digital image steganography products that meet militarily needs continue to appear in the open market. If COTS products can meet a military requirement, adopting and integrating these COTS products is less expensive than building custom products and could eliminate some of the need for inventory, depot storage, and related life-cycle costs. However, the cost of additional staff to manage and maintain the steganographic functionality for large complex systems could be a significant cost issue. Most of the functionality can be automated; however, there are still potentially expensive requirements to recruit and retain technically qualified, trustworthy, and responsible personnel to operate, manage, and support the required end-user training, standardization, and T&E programs required for optimum information system security.

BACKGROUND

Image steganography can be used to conceal an encrypted message. The technique of combining image steganography and encryption or multiple-encryption could present a challenge to National Security and law

[97] These statistical and human sensory threshold specifications are different and evolving for each technique and form of digital media (text, audio, and video files).

[98] Binary executable files also can be encoded but at a lower rate. The Hydan technique substitutes functionally equivalent op-codes. See http://crazyboy.com/hydan/.

enforcement agency cryptanalysts. Even if a message were known to exist in an electronic image, the message bits would have to be identified and isolated for cryptanalysis. This process could make plaintext recovery time-consuming, if not impracticable. Steganography can various forms that are not strictly digital image steganography. Banks make use of a code-word execution technique when they need to send highly secure “action” messages to execute preplanned actions. Predetermined and mutually agreed actions are then set in motion, with instructions implicit in one short phrase embedded in routine banking message traffic.